COMODO
Creating Trust Online™

Scan Report Executive Summary

Part 1. Scan Information

Scan Customer Company:	rsync.net	ASV Company:	Comodo CA Limited
Date scan was completed:	06-09-2015	Scan expiration date:	09-07-2015

Part 2. Component Compliance Summary

IP Address : 64.62.236.70 Pass Fail

Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
64.62.236.70	SSH Weak MAC Algorithms Enabled ssh (2222/tcp)	Low	2.6	Pass	The vulnerability is not included in the NVD
64.62.236.70	SSH Server CBC Mode Ciphers Enabled ssh (2222/tcp) CVE-2008-5161	Low	2.6	Pass	
64.62.236.70	SSH Weak MAC Algorithms Enabled ssh (22/tcp)	Low	2.6	Pass	The vulnerability is not included in the NVD
64.62.236.70	SSH Server CBC Mode Ciphers Enabled ssh (22/tcp) CVE-2008-5161	Low	2.6	Pass	
64.62.236.70	FTP Supports Clear Text Authentication ftp (21/tcp)	Low	2.6	Pass	The vulnerability is not included in the NVD
64.62.236.70	SSH Algorithms and Languages Supported ssh (2222/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	SSH Protocol Versions Supported ssh (2222/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	SSH Server Type and Version Information ssh (2222/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD

IP Address	Vulnerabilities Noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives or Compensating Controls Noted by ASV for this Vulnerability
64.62.236.70	Service Detection ssh (2222/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	Nessus TCP scanner ssh (2222/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	SSH Algorithms and Languages Supported ssh (22/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	SSH Protocol Versions Supported ssh (22/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	SSH Server Type and Version Information ssh (22/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	Service Detection ssh (22/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	Nessus TCP scanner ssh (22/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	FTP Server Detection ftp (21/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	Service Detection ftp (21/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	Nessus TCP scanner ftp (21/tcp)	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	Device Type general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	Common Platform Enumeration (CPE) general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	OS Identification general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD
64.62.236.70	TCP/IP Timestamps Supported general/tcp	Low	0.0	Pass	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.
Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.
Protect your target with an IP filter.
Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.

Part 3b. Special notes by IP Address

IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not	Scan customer's description of actions taken to either: 1)remove the software or 2) implement security controls to secure the
64.62.236.70	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Access: ssh (2222/tcp)		
64.62.236.70	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Access: ssh (22/tcp)	The customer declares the software is implemented securely.	